[1], Adversarial Machine learning technique used to deceive the Deep Learning (DL) based NIDS that made DL-NIDS a vulnerable. So, instead of securing the network, the network will become more vulnerable due to deep learning infrastructure. There are two methods to secure deep learning models i.e. reactive and proactive. Defensive distillation and adversarial training are two proactive techniques while Pixel Defense is an example of reactive defense. An Open Source library Cleverhans is available for adversarial training. False positives detection increases the reliability of system while false negatives show the efficiency of system. There is a tradeoff between both of these values. There are two adversarial attacking objectives i.e. integrity violation exploited by false negative and availability violations exploited by false positive.

[2], NIDS are basically of 2 types: Signature based NIDS (SNIDS) and Anomaly Detection based NIDS (ADNIDS). SNIDS used for detecting the intrusion based on known features while ADNIDS is used for detecting unknown featured intrusions. In this paper, Self-Taught Learning (STL) and Non-symmetric Deep Auto-Encoder(NSDA) is used to learn patterns in unsupervised learning. Sparse auto-encoder will be used to learn the unknown patterns and then logistic regression function will be used to classify the user behavior learned by stack autoencoder. There are already many NIDS researched and implemented but a real time and more generic NIDS requires a lot of work yet. Total 115 features are considered here that are given as input to neural network. Deep network is made by stacking the autoencoders and logistic regression function is used to classify user as an intruder or normal user.

[3],This paper presents a novel deep learning technique for intrusion detection. Nonsymmetric deep autoencoder (NDAE) for unsupervised feature learning is proposed in this paper. This has been implemented using GPU enabled Tensor Flow with datasets KDD Cup ‘99 and NSL-KDD datasets. Most solutions are signature-based rather than anomaly based. Where signature based solutions are those solutions that detect an attack which is known .i.e. it belongs to a library/dataset of known attacks. On the other hand Behaviour or anomaly based as the name suggest is based upon the pattern of normal behaviour .i.e whenever an odd behaviour over a machine is observed the indication is made. Cetainly , the volume and diversity of network data is a challenge. However, here deep and shallow learning techniques are deployed. Particularly, Random Forest and NDAE are used. This paper focuses on nonsymetric data dimentionality reduction. For data dimensionality reduction the technique used is auto encoder. The input is first transformed into a typically lower-dimensional space (encoder), and then expanded to reproduce the initial data (decoder). Once a layer is trained, its code is fed to the next, to better model highly non-linear dependencies in the input. This paradigm focuses on reducing the dimensionality of input data. To achieve this, there is a special layer - the code layer , at the centre of the deep auto-encoder structure. This code layer is used as a compressed feature vector for classification or for combination within a stacked auto-encoder. If applied deeplearning to autoencoders it is termed as deep auto encoders or Stacked auto encoders. As for this paper NDAE Non symmetric deep auto encoder is used. Which learns the important features using similar strategy to that of deep auto encoder. Hidden input vector is given by hi = σ(Wi . hi−1 + bi) and “sigmoid function” is used for computing the actual output. To learn more complex features Stacked NDAE may be used. The stacked auto encoders with soft-max layer is not good at classification as compared to other classification algorithms so here stacked NDAE with shallow learning classifier is opted, .i.e Random Forest Classifier Algorithm.

[1] 27 March,2019. Link: <https://arxiv.org/pdf/1903.11688.pdf>

[2] March 2019. Link: <https://search.proquest.com/openview/ab6d5a2cbbb23e2c3cc10af0093a3134/1?pq-origsite=gscholar&cbl=2026671>

[3] February 2018: <https://blogs.qub.ac.uk/netsec/wp-content/uploads/sites/153/2019/02/08264962.pdf>